UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

SPEECH TRANSCRIPTION, LLC, Plaintiff, v. CISCO SYSTEMS, INC. Defendant.	§ § § § § § § § §	Civil Action No. 6:23-CV-376-AM

CISCO SYSTEMS INC.'S MOTION TO DISMISS THE COMPLAINT OF SPEECH TRANSCRIPTION, LLC PURSUANT TO FED. R. CIV. P. 12(C)

TABLE OF CONTENTS

Page(s)

I. INTRODUCTION 1

II. LEGAL STANDARD 2

A. *Alice* Prohibits Patenting Claims That Merely Require Generic Computer Implementation of An Abstract Idea 2

B. Rule 12(c) Motion for Judgment on the Pleadings 4

C. Direct and Indirect Patent Infringement 4

III. STATEMENT OF FACTS 6

IV. ARGUMENT 10

A. The Asserted Patent is Directed to Ineligible Subject Matter 10

1. Alice Step One 10

2. Alice Step Two 13

B. Plaintiff Makes No Plausible Allegations of Direct Infringement 14

1. Plaintiff Does Not Allege Cisco "Makes," "Uses," or "Sells" Any Infringing Product or Thing 15

2. Direct Infringement of a System Claim Cannot Be Satisfied by Different Parties 17

3. The Assortment of Other Cisco Products Cited in the Claim Chart Are Irrelevant 17

C. Plaintiff's Claims for Pre-Suit Indirect Infringement Should be Dismissed 20

V. CONCLUSION 20

TABLE OF AUTHORITIES

Page(s)

Cases

Affinity Labs of Tex., LLC v. Amazon.com, Inc.,
838 F.3d 1266 (Fed. Cir. 2016).....3, 12

AlexSam, Inc. v. Aetna, Inc.,
No. 3:19-CV-01025 (VAB), 2020 WL 5502323 (D. Conn. Sept. 11, 2020).....5

Alice Corp. Pty. v. CLS Bank International,
573 U.S. 208 (2014)..... *passim*

Ashcroft v. Iqbal,
556 U.S. 662 (2009).....4

BillJCo, LLC v. Apple Inc.,
583 F. Supp. 3d 769 (W.D. Tex. 2022).....20

Bot M8 LLC v. Sony Corp. of Am.,
4 F.4th 1342 (Fed. Cir. 2021) 17

Bowlby v. City of Aberdeen,
681 F.3d 215 (5th Cir. 2012) 4

BSG Tech LLC v. Buyseasons, Inc.,
899 F.3d 1281 (Fed. Cir. 2018).....3

CardioNet, LLC v. InfoBionic, Inc.,
955 F.3d 1358 (Fed. Cir. 2020).....2

Centillion Data Sys. LLC v. Qwest Commc'ns Int'l Inc.,
631 F.3d 1279 (Fed. Cir. 2011)..... *passim*

Chhim v. Univ. of Tex. At Austin,
836 F.3d 467 (5th Cir. 2016) 17

Commil USA, LLC v. Cisco Sys., Inc.,
135 S. Ct. 1920 (2015).....5

CosmoKey Sols. GmbH & Co. KG,
15 F.4th at 1096-97 14

Credit Acceptance Corp. v. Westlake Servs.,
859 F.3d 1044 (Fed. Cir. 2017).....11

Customedia Techs., LLC v. Dish Network Corp.,
951 F.3d 1359 (Fed. Cir. 2020).....12

cxLoyalty, Inc. v. Maritz Holdings Inc.,
986 F.3d 1367 (Fed. Cir. 2021).....10

De La Vega v. Microsoft Corp.,
No. W-19-CV-00612-ADA, 2020 WL 3528411 (W.D. Tex. Feb. 11, 2020).....5, 15, 20

Doe v. MySpace, Inc.,
528 F.3d 413 (5th Cir. 2008) 4

DSU Med. Corp. v. JMS Co.,
471 F.3d 1293 (Fed. Cir. 2006).....5

Dynacore Holdings Corp. v. U.S. Philips Corp.,
363 F.3d 1263 (Fed. Cir. 2004).....16

e-Numerate Sols., Inc. v. United States,
149 Fed. Cl. 563 (2020) 11

Elec. Power Grp., LLC v. Alstom S.A.,
830 F.3d 1350 (Fed. Cir. 2016).....10

FairWarning IP, LLC v. Iatric Sys., Inc.,
839 F.3d 1089 (Fed. Cir. 2016).....4, 11

Free Stream Media Corp. v. Alphonso Inc.,
996 F.3d 1355 (Fed. Cir. 2021).....13

Global-Tech Appliances, Inc. v. SEB S.A.,
563 U.S. 754 (2011).....6

Halo Elecs., Inc. v. Pulse Elecs., Inc.,
579 U.S. 93 (2016).....6

Intellectual Ventures I LLC v. Motorola Mobility LLC,
870 F.3d 1320 (Fed. Cir. 2017).....5

Iron Oak Techs., LLC v. Acer Am. Corp.,
No. 6:17-cv-00143-RP-JCM, 2017 WL 9477677 (W.D. Tex. Nov. 28, 2017) 6

Kewanee Oil Co. v. Bicron Corp.,
416 U.S. 470 (1974).....12

Lone Star Fund V (U.S.) L.P. v. Barclays Bank PLC,
594 F.3d 383 (5th Cir. 2010) 4

Loyalty Conversion Sys. Corp. v. Am. Airlines, Inc.,
66 F. Supp. 3d 829 (E.D. Tex. 2014) 4

Lyda v. CBS Corp.,
838 F.3d 1331 (Fed. Cir. 2016) 5

Mosaic Brands v. Ridge Wallet LLC,
2020 WL 5640233 (C.D. Cal. Sept. 3, 2020) 20

Network Architecture Innovations LLC v. CC Network Inc.,
2017 WL 1398276 (E.D. Tex. Apr. 18, 2017) 4

NexusCard, Inc. v. Kroger Co.,
173 F. Supp. 3d 462 (E.D. Tex. 2016), *aff'd*, 688 F. App'x 916 (Fed. Cir. 2017) 11

Parity Networks, LLC v. Cisco Sys., Inc.,
No. 6:19-cv-209-ADA, 2019 WL 3940952 (W.D. Tex. July 26, 2019) 6

Parus Holdings Inc. v. Sallie Mae Bank,
137 F. Supp. 3d 660 (D. Del. 2015), *aff'd*, 677 F. App'x 682 (Fed. Cir. 2017) 14

Qwikcash, LLC v. Blackhawk Network Holdings, Inc.,
No. 4:19-CV-876-SDJ, 2020 WL 6781566 (E.D. Tex. Nov. 17, 2020) 6

Ruby Sands LLC v. Am. Nat'l Bank of Tex.,
2:15-cv-1955-JRG, 2016 WL 3542430 (E.D. Tex. June 28, 2016) 5, 17, 19, 20

SAP Am., Inc. v. InvestPic, LLC,
898 F.3d 1161 (Fed. Cir. 2018) 13

SAP Am., Inc. v. InvestPic, LLC,
898 F.3d 1166 (Fed. Cir. 2018) 3

Secured Mail Sols., LLC v. Universal Wilde, Inc.,
873 F.3d 905 (Fed. Cir. 2017) 3

Simio, LLC v. FlexSim Software Prods., Inc.,
983 F.3d 1353 (Fed. Cir. 2020) 12, 13

Taylor v. Books A Million, Inc.,
296 F.3d 376 (5th Cir. 2002) 17

Trading Techs. Int'l, Inc. v. IBG LLC,
921 F.3d 1378 (Fed. Cir. 2019) 3

Universal Secure Registry LLC v. Apple Inc.
10 F.4th 1342 (Fed. Cir. 2021), *cert. denied*, 212 L. Ed. 2d 778, 142 S. Ct. 2707 (2022).....11, 12, 14

Vervain, LLC v. Micron Tech., Inc.,
2022 WL 23469 (W.D. Tex. Jan. 3, 2022) 17, 19

Statutes

35 U.S.C. § 101.....2, 10, 12

35 U.S.C. § 271(a) 5, 14, 16

35 U.S.C. § 271(b).....5

35 U.S.C. § 271(c) 6

35 U.S.C. § 286.....18

Other Authorities

Fed. R. Civ. P. 8(a) 5

Fed. R. Civ. P. 12.....4, 12, 13

Fed. R. Civ. P. 12(b)(6).....4

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

SPEECH TRANSCRIPTION, LLC, Plaintiff, v. CISCO SYSTEMS, INC. Defendant.	§ § § § § § § § §	Civil Action No. 6:23-CV-376

CISCO SYSTEMS INC.'S MOTION TO DISMISS THE COMPLAINT OF SPEECH TRANSCRIPTION, LLC PURSUANT TO FED. R. CIV. P. 12(C)

I. INTRODUCTION

This Complaint alleges the infringement of a patent directed to a network security system that receives and executes security software from multiple vendors. The claims of the asserted patent are directed to nothing more than the abstract idea of a computer-implemented intermediary to receive and execute security software from multiple vendors. As a result, the claims are patent-ineligible under *Alice Corp. Pty. v. CLS Bank International*, 573 U.S. 208 (2014) and its progeny.

Further, Cisco Systems, Inc. ("Cisco") does not design or sell network security architectures. Cisco does not, and Plaintiff Speech Transcription, LLC ("Speech Transcription" or "Plaintiff") cannot plausibly allege, that Cisco provides a "unified security management system" for its customers as is alleged in the Complaint. Instead, Plaintiff provides a conclusory claim chart alleging infringement of a single system claim by stitching together screen captures from Cisco's marketing documents outlining generalized network design principles under the umbrella term "Cisco SAFE." But Cisco SAFE is not a product—it is a set of generic and non-specific guidelines, references, and organizational frameworks *that third parties can use* to design secure networks.

None of the cited Cisco documents identify any actual product (or bundle of products) offered by Cisco, let alone a product that can plausibly be alleged to satisfy each limitation of the asserted claim. Plaintiff points either to hypothetical, fictitious business entities or to unexplained "agents," and not to Cisco, as responsible for satisfying the elements of the charted system claim. But infringement of a system claim cannot be divided between multiple parties. In the absence of an allegation of infringement by a Cisco product, Plaintiff's allegations of direct infringement must be dismissed with prejudice.

Plaintiff's claims of indirect infringement, both inducement and contributory, and its claim for willful infringement, fare no better. The Complaint contains no specific allegations to plausibly support Plaintiff's claims of indirect infringement, but only conclusory statements. And Plaintiff additionally fails to plead any pre-suit knowledge, as necessary to support a claim of willful infringement. These indirect infringement claims must also be dismissed with prejudice.

II. LEGAL STANDARD

A. *Alice* Prohibits Patenting Claims That Merely Require Generic Computer Implementation of An Abstract Idea

In defining subject matter eligible for patenting, 35 U.S.C. § 101 contains "an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable." *Alice*, 573 U.S. at 216. Section 101 prohibits patenting claims "which merely require generic computer implementation" of an abstract idea. *Id.* at 221. In *Alice*, the Supreme Court set forth a two-step test for determining whether a claim is directed to such ineligible subject matter.

***Alice* step one.** The first step is to "determine whether the claims at issue are directed to one of those patent-ineligible concepts," *e.g.*, an abstract idea. *Id.* at 217. "*Alice* step one presents a legal question that can be answered based on the intrinsic evidence" and "does not require an evaluation of the prior art or facts outside of the intrinsic record." *CardioNet, LLC v. InfoBionic,*

Inc., 955 F.3d 1358, 1372 (Fed. Cir. 2020). "Under this inquiry, [courts] evaluate the focus of the claimed advance over the prior art to determine if the character of the claim as a whole, considered in light of the specification, is directed to excluded subject matter." *Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378, 1384 (Fed. Cir. 2019) (quotation omitted). Where a claim recites "a desired function or outcome, without providing any limiting detail that confines the claim to a particular solution to an identified problem," the "functional nature of the claim confirms that it is directed to an abstract idea." *Affinity Labs of Tex., LLC v. Amazon.com, Inc.*, 838 F.3d 1266, 1269 (Fed. Cir. 2016).

***Alice* step two.** If a claim is directed to ineligible subject matter, the second step is to "determine whether [any] additional elements transform the nature of the claim into a patent-eligible application" by reciting "an inventive concept—*i.e.*, an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself." *Alice*, 573 U.S. at 217–18 (quotations omitted). Even if "the techniques claimed are groundbreaking, innovative, or even brilliant, [] that is not enough for eligibility" if "the advance lies entirely in the realm of abstract ideas." *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1166, 1163 (Fed. Cir. 2018). "What is needed is an inventive concept in the non-abstract application realm." *Id.* at 1168. The "inquiry is not whether the claimed invention as a whole is unconventional or non-routine," but "whether the claim limitations other than the invention's use of the ineligible concept to which it was directed were well-understood, routine and conventional." *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018).

The two-step *Alice* inquiry is a legal one, which may be decided based on the "intrinsic evidence from the specification without need for 'extraneous fact finding outside the record.'" *Secured Mail Sols., LLC v. Universal Wilde, Inc.*, 873 F.3d 905, 912 (Fed. Cir. 2017) (internal

citation omitted). Accordingly, this Court, like many others, has addressed patent eligibility at the Rule 12 stage. *See Loyalty Conversion Sys. Corp. v. Am. Airlines, Inc*., 66 F. Supp. 3d 829, 847 (E.D. Tex. 2014); *Network Architecture Innovations LLC v. CC Network Inc.*, 2017 WL 1398276, at *7 (E.D. Tex. Apr. 18, 2017); *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1097 (Fed. Cir. 2016).

B. Rule 12(c) Motion for Judgment on the Pleadings

"A motion for judgment on the pleadings under Rule 12(c) is subject to the same standard as a motion to dismiss under Rule 12(b)(6)." *Doe v. MySpace, Inc.*, 528 F.3d 413, 418 (5th Cir. 2008). To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is not plausible unless the "plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*. (citing *Twombly*, 550 U.S. at 556). In making this assessment, courts may consider "the complaint, any documents attached to the complaint, and any documents attached to the motion to dismiss that are central to the claim and referenced by the complaint." *Lone Star Fund V (U.S.) L.P. v. Barclays Bank PLC*, 594 F.3d 383, 387 (5th Cir. 2010). The court must then decide whether those facts state a claim for relief that is plausible on its face. *Bowlby v. City of Aberdeen*, 681 F.3d 215, 219 (5th Cir. 2012). But courts "are not bound to accept as true a legal conclusion couched as a factual allegation," and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice" to meet the plausibility standard. *Ashcroft*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 555).

C. Direct and Indirect Patent Infringement

To state a claim for direct infringement, a plaintiff must explicitly plead facts to plausibly

support the assertion that a defendant "without authority makes, uses, offers to sell, or sells any patented invention…during the term of the patent." 35 U.S.C. § 271(a); *see also* Fed. R. Civ. P. 8(a); *Ruby Sands LLC v. Am. Nat'l Bank of Tex.*, 2:15-cv-1955-JRG, 2016 WL 3542430, at *2 (E.D. Tex. June 28, 2016). The Federal Circuit has recognized that its "cases have applied joint infringement to method claims and *not system claims*." *See Lyda v. CBS Corp.*, 838 F.3d 1331, 1339 (Fed. Cir. 2016) (emphasis added) (citing *Centillion Data Sys. LLC v. Qwest Commc'ns Int'l Inc.*, 631 F.3d 1279, 1284 (Fed. Cir. 2011)). Instead, "direct infringement by use of a system claim requires a party ... to use each and every ... element of a claimed system." *Centillion*, 631 F.3d at 1284 (internal quotation marks and brackets omitted); *Intellectual Ventures I LLC v. Motorola Mobility LLC*, 870 F.3d 1320, 1328 (Fed. Cir. 2017). "[T]o use a system for purposes of infringement, a party must put the invention into service, *i.e.*, control the system as a whole and obtain benefit from it." *Id*. (internal quotation marks and citation omitted). When the complaint fails to allege that the defendant uses (for system claims) or controls (for method claims) each element of the claim, claims of direct infringement are not plausible and should be dismissed. *See De La Vega v. Microsoft Corp.*, No. W-19-CV-00612-ADA, 2020 WL 3528411, at *7 (W.D. Tex. Feb. 11, 2020); *AlexSam, Inc. v. Aetna, Inc.,* No. 3:19-CV-01025 (VAB), 2020 WL 5502323, at *15 (D. Conn. Sept. 11, 2020).

To succeed on a claim of induced infringement, a plaintiff must allege facts showing that defendant: (1) had actual knowledge of the patent; (2) actively and knowingly aided and abetted a third-party to directly infringe the patent; and (3) had specific intent and action to induce infringement. *See DSU Med. Corp. v. JMS Co.*, 471 F.3d 1293, 1305 (Fed. Cir. 2006); *see also Commil USA, LLC v. Cisco Sys., Inc.*, 135 S. Ct. 1920, 1926 (2015). The Supreme Court has held that "induced infringement under § 271(b) requires knowledge that the induced acts constitute

patent infringement." *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 766 (2011).

To succeed on a contributory infringement claim, Plaintiff must allege facts showing that defendant: (1) directly infringed, (2) had knowledge of the patent, (3) that the component has no substantial non–infringing uses, and (4) that the component is a material part of the invention. *See* 35 U.S.C. § 271(c); *Iron Oak Techs., LLC v. Acer Am. Corp.*, No. 6:17-cv-00143-RP-JCM, 2017 WL 9477677, at *6-7 (W.D. Tex. Nov. 28, 2017). Of course, a claim for either induced or contributory infringement also requires an underlying act of direct infringement. *See Qwikcash, LLC v. Blackhawk Network Holdings, Inc.*, No. 4:19-CV-876-SDJ, 2020 WL 6781566, at *5 (E.D. Tex. Nov. 17, 2020) ("Where a plaintiff has not adequately pleaded an underlying act of direct infringement, theories of indirect infringement must be dismissed.").

Finally, to demonstrate willful infringement, a plaintiff must show "[t]he sort of conduct warranting enhanced damages has been variously described ... as willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or—indeed—characteristic of a pirate." *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, 579 U.S. 93, 103-04 (2016). To sufficiently plead willful infringement, "a plaintiff must allege facts plausibly showing that as of the time of the claim's filing, the accused infringer: (1) knew of the patent-in-suit; (2) after acquiring that knowledge, it infringed the patent; and (3) in doing so, it knew, or should have known, that its conduct amounted to infringement of the patent." *Parity Networks, LLC v. Cisco Sys., Inc*., No. 6:19-cv-209-ADA, 2019 WL 3940952, at *3 (W.D. Tex. July 26, 2019) (citations omitted).

III. STATEMENT OF FACTS

Speech Transcription's Complaint alleges that Cisco "sells, advertises, offers for sale, uses, or otherwise provides exemplary products, including at least the Cisco SAFE architecture" as infringing at least Claim 14 of U.S. Patent No. 8,938,799 (the "'799 Patent" or "Asserted Patent"). *See* Dkt. 1, ¶ 27. The Complaint does not name any actual Cisco product as infringing, but instead

points to the term "Cisco SAFE" as used in Cisco's marketing documents as the "exemplary product." *Id*. Plaintiff's infringement chart relies exclusively on out-of-context excerpts from two Cisco documents. The first is a 2010 document titled "SAFE Overview Guide" ("SAFE Overview Guide"), which is attached as Exhibit 1 to this brief. *See* Ex. 1. The second document is Chapter 11 from a 2010 document titled "Cisco SAFE Reference Guide" ("SAFE Reference Guide") attached as Exhibit 2 to this brief. *See* Ex. 2.

Critically, as Plaintiff's cited documents indicate, Cisco SAFE is not a product. Rather, Cisco SAFE is a "reference model" which "provides guidance to common business functions that require security capabilities." *See* Ex. 1 at 6. "Cisco SAFE" refers to a set of design principles, best practices, and organizational framework for approaching network security. *See id*. ("SAFE is not a single answer. The model is a reference for common threats, risks, and policies across the business of a company."); *see also* Ex. 2 at 1-1 (executive summary stating that "Cisco SAFE provides the design and implementation guidelines for building secure and reliable network infrastructures…"). Plaintiff's cited documents only confirm that Cisco does not sell "Cisco SAFE" either as a standalone product or as a bundle of individual Cisco products.

Plaintiff attaches an infringement chart attempting to map system Claim 14 of the '799 Patent to marketing documents referencing Cisco SAFE. The text of Claim 14 is provided below with relevant text bolded:

Claim 14	
Preamble	A **security subsystem** configurable between **a network** and **a host of an endpoint**, the security subsystem comprising computing resources for providing:
Limitation (a)	an **open platform** for **receiving and executing security function software modules** from **multiple vendors** for providing defense functions for protection of the host.

The preamble of Claim 14 recites "[a] security subsystem configurable between a network

and a host of an endpoint [i.e., a laptop or smartphone]" comprising functionalities addressed in subsequent limitation (a). For this preamble, Plaintiff's claim chart relies general statements describing Cisco SAFE as "security reference architecture" that "logically maps business flows to security capabilities" and "help[s] you design a secure infrastructure," as well as Figures 28 and 3 of the SAFE Overview Guide, though relevant portions of Figure 3 were cropped in the claim chart. Those two figures are provided in full at Exhibit 3 to this motion. *See* Ex. 3.

Plaintiff also relies on portions of the document stating that Cisco SAFE design principles are "compatible" with various products that Cisco offers, like CS-MARS or CSM. Dkt. 1-2 at 1. But as the document indicates, these Cisco products provide, at best, individual security functions, and not the "unified security system" recited by the claims. Dkt. 1-2 at 5. Plaintiff's attempt to incorporate these unrelated products does not overcome the fundamental flaw in its infringement allegations – SAFE's design principles are not a product, but rather a design framework *that customers can use to design their own security systems*. *See e.g.*, Ex. 1 at 6; Ex. 2 at 1-1. As the home page for Cisco SAFE explains: "This Cisco security reference architecture features easy-to-use visual icons that help you design a secure infrastructure for the edge, branch, data center, campus, cloud, and WAN. The framework encompasses operational domains such as management, security intelligence, compliance, segmentation, threat defense, and secure services." Ex. 4 (home page for Cisco SAFE). In other words, Cisco SAFE cannot be a "security subsystem;" it is simply a design tool that allows third-parties to design their network security architectures in accordance with industry best-practices and with each business's specific needs.

Limitation (a) similarly recites a physical element: "an open platform" that "execute[es] security function software modules from multiple vendors for providing defense functions for protection of the host." Dkt. 1-2 at 5. But to satisfy this limitation, Plaintiff once again relies on

depictions of the Cisco SAFE reference architecture – which is not an actual "platform" or "device," but simply an approach to network design that third-parties may adopt. Citing Figure 1 (reproduced below), Plaintiff's claim chart states that "business flows are analyzed to determine required security capabilities, which demonstrate protection of host of an endpoint." But this figure does not identify any actual Cisco product that would serve as the "open platform." *Id*. at 6.

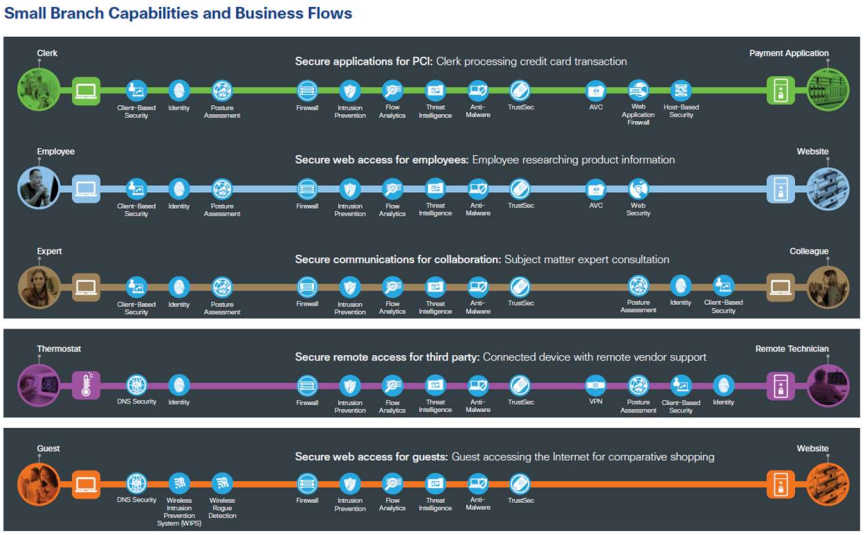

Figure 1 *In the capability phase, business flows are analyzed to determine the required security capabilities.*

The claim chart further attempts to incorporate unrelated Cisco products by alleging that an "agent of Cisco SAFE checks the operation against the security policy for threats." Dkt. 1-2 at 5. According to the Complaint, this purported "agent" of Cisco SAFE is CSA (Cisco Security Agent) "which provides defense-in-depth protection…by combining security policies," defined as "collections of rules that IT or security administrators assign to protect servers and desktops," for businesses. *Id*. But Plaintiff's claim chart provides no basis at all for concluding that CSA or SAFE provides a platform for integrating security modules from different vendors as required by Limitation (a).

IV. ARGUMENT

A. The Asserted Patent is Directed to Ineligible Subject Matter

The sole claim charted in the complaint – Claim 14 – is patent-ineligible under *Alice Corp. Pty. v. CLS Bank International*, 573 U.S. 208 (2014) and its progeny.

1. Alice Step One

The '799 Patent contains only a single asserted independent claim, Claim 14, which is the sole claim charted in Plaintiff's complaint. Claim 14 recites nothing more than the abstract idea of an intermediary platform for receiving and executing security software modules from multiple vendors. The preamble of claim 14 recites a "security subsystem configurable between a network and a host of an endpoint." '799 Patent at 19:47-52. The security system – *i.e.*, the apparatus of the claim – is defined only in terms of the function that it performs: it is configured for "receiving and executing security functions software modules from multiple vendors for providing defense functions for protection of the host." *Id*. The use of this type of "result-focused, functional character of claim language . . . has been a frequent feature of claims held ineligible under § 101." *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1356 (Fed. Cir. 2016); *see also cxLoyalty, Inc. v. Maritz Holdings Inc.*, 986 F.3d 1367, 1380 (Fed. Cir. 2021) (holding as patent-ineligible a claim for a "platform" which "provides the ability for a participant to use a single loyalty program GUI to make points-based purchases directly from multiple third-party vendor systems via multiple APIs.").

The "security sub-system" containing an "open platform" is directed to nothing more than the abstract idea of integrating and managing tools from multiple sources. The claimed system situated "between a network and a host of an endpoint" facilitates exchanges of information between a host system (i.e., corporate or residential users) and vendor systems. '799 Patent at 19:47-52. In Plaintiff's own words, the system of Claim 14 "protect[s] endpoint computing

systems" by "managing, providing, and obtaining security functions." Dkt. 1, ¶ 14.

The security subsystem described in Claim 14 amounts to no more taking security tools from multiple sources and combining them into one "open platform," which is inherently abstract. "The mere combination of []sources, however, does not make the claims patent eligible." *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1096–97 (Fed. Cir. 2016). The abstract idea described in Claim 14 is analogous to a toolbox containing various tools such as a hammer, screwdriver, and saw. Each tool may come from a different source – a hammer from Craftsmen, a screwdriver from DeWALT, and a saw from Makita – and may perform a different function. But even if someone takes these tools and combines them in a single toolbox, the system is merely a result of applying the abstract idea of combining existing sources into a single package without altering the features of any individual tool. *See e-Numerate Sols., Inc. v. United States*, 149 Fed. Cl. 563, 584 (2020) ("The mere combination of data sources, however, does not make the claims patent eligible"); *NexusCard, Inc. v. Kroger Co.*, 173 F. Supp. 3d 462, 467 (E.D. Tex. 2016), *aff'd*, 688 F. App'x 916 (Fed. Cir. 2017) ("[D]escribing two abstract ideas in connection with each other…does not cause either abstract idea to then become a concrete thing."); *see also Credit Acceptance Corp. v. Westlake Servs., 859 F.3d 1044, 1055–56 (Fed. Cir. 2017) (*holding that claims directed to "configuring a computer system to combine data from multiple electronic data sources" are inherently abstract).

The claim at issue here is akin to those held ineligible in *Universal Secure Registry LLC v. Apple Inc*. 10 F.4th 1342, 1353 (Fed. Cir. 2021), *cert. denied*, 212 L. Ed. 2d 778, 142 S. Ct. 2707 (2022). There, the Federal Circuit analyzed the patentability of a system which combined multiple existing security techniques including biometric authentication, multi-factor authentication, and authentication using multiple devices to verify the identity of a user in financial transactions. *Id*.

The Federal Circuit found that the patent claims were directed to the abstract idea of combining multiple conventional authentication techniques, and that simply combining the tools into a single package is abstract absent any novel elements or additional functionality of any of the individual tools. *Id*. (finding the claimed system unpatentable as "merely a combination of known authentication techniques that yields only expected results.").

Plaintiff's conclusory allegation that the claims of the '799 Patent "comprise non-conventional approaches that transform the inventions as claimed into substantially more than mere abstract ideas" and "are not drawn . . . to abstract ideas" cannot save the claims. Conclusory allegations are given no weight in Section 101 analysis at the Rule 12 stage. *Simio, LLC v. FlexSim Software Prods., Inc.*, 983 F.3d 1353, 1365 (Fed. Cir. 2020).

And even a novel combination of abstract elements alone is not sufficient to make otherwise abstract ideas patentable. "[N]o patent is available…however useful, novel, and nonobvious, unless it falls within one of the express categories of patentable subject matter." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 483 (1974). "In addressing the first step of the section 101 inquiry, as applied to a computer-implemented invention," it is important "to ask whether the claims are directed to 'an improvement in the functioning of a computer,' or merely 'adding conventional computer components to well-known business practices.'" *Affinity Labs of Tex., LLC*, 838 F.3d at 1270 (quoting *Enfish, LLC v. Microsoft Corp*., 822 F.3d 1327, 1338 (Fed. Cir. 2016)). Claim 14 of the '799 Patent cannot claim any such improvement because it simply discusses the integration of multiple security software "modules" without any actual improvement of the underlying technology beyond the implementation of computer-based tools used to combine well-known security "security modules" offered by other vendors. *See Customedia Techs., LLC v. Dish Network Corp*., 951 F.3d 1359, 1364 (Fed. Cir. 2020) (holding that eligible subject-matter in

this context "require[s] the claims to be directed to an improvement in the functionality of the computer or network platform itself.").

2. Alice Step Two

Asserted Claim 14 also fails at *Alice* step two because no inventive concept can be identified in the claim. As an initial matter, Plaintiff's conclusory allegation that the '799 Patent contains "inventive concepts which transform the underlying non-abstract aspects of the claims into patent-eligible subject matter" (Dkt. 1, § 21) cannot help it survive a Rule 12 challenge. Federal Circuit precedent requires those allegations be given no weight. *Simio*, 983 F.3d at 1365.

And while the Complaint alleges that "conventionally, the deployment of defense functions in enterprise networks can be network-based or host-based, or both," and that "host-based [immunization] … requires an agent to be installed in each host," and that "deployed security infrastructure consisting of multiple defense and immunization functions may burden the host." Dkt. 1, ¶ 15. Setting aside that these allegations contain no factual support, the only proposed solution is the abstract idea of putting the various defense software and immunization functions into an "open platform." Where, as here, the supposed inventive concept is wholly in the realm of the abstract, the claims do not contain an inventive concept and cannot survive at *Alice* Step Two. *See SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1170 (Fed. Cir. 2018) (finding claim ineligible at *Alice* Step Two because "[t]here is, in short, nothing 'inventive' about any claim details, individually or in combination, that are not themselves in the realm of abstract ideas.").

In addition, Claim 14 only recites generic and conventional computer components (i.e., 'computing resources,' 'network,' and 'endpoint') and functionality for carrying out the abstract idea of combining of well-known and non-novel tools offered by others. *See e.g., Free Stream Media Corp. v. Alphonso Inc.*, 996 F.3d 1355, 1366 (Fed. Cir. 2021) (holding "the claimed

elements … comprise generic computing components—e.g., 'servers'—arranged in a conventional manner and thus do[] not transform the claim into something other than the abstract idea"). Notably, nowhere does Claim 14 recite any computer or software that is an advance over conventional technology. *Parus Holdings Inc. v. Sallie Mae Bank*, 137 F. Supp. 3d 660, 674 (D. Del. 2015), *aff'd*, 677 F. App'x 682 (Fed. Cir. 2017) (finding the claims at issue lacked an inventive concept because they were not sufficiently specific and did not "reference any customization" of the hardware and software described in the claims).

And Claim 14 does not recite any unique security methods, but rather, an "open platform" to aggregate already known methods, *i.e.*, a toolbox. This claimed combination recites nothing more than the "combination of long-standing conventional methods" for security which would "yield[] expected results of an additive increase in security" from each individual vendor's module. *Universal Secure Registry LLC*, 10 F.4th at 1353. While "[i]mproving security … can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem," and nothing in the record suggests such a technological improvement. *CosmoKey Sols. GmbH & Co. KG v. Duo Sec. LLC*, 15 F.4th 1091, 1096–97 (Fed. Cir. 2021). "There is nothing in the specification suggesting, or any other factual basis for a plausible inference (as needed to avoid dismissal), that the claimed combination of these conventional [] techniques achieves more than the expected sum of the security provided by each technique." *Universal Secure Registry LLC*, 10 F.4th at 1353. There is nothing in Claim 14 that can save it at *Alice* Step Two.

B. Plaintiff Makes No Plausible Allegations of Direct Infringement

To properly plead infringement against Cisco, there must be some plausible allegation that Cisco "makes, uses, offers to sell, or sells" the patented invention. 35 U.S.C. § 271(a). "In order to 'make' the system under § 271(a), [a defendant] would need to combine all of the claim

elements." *Centillion*, 631 F.3d at 1288. Similarly, "[t]o 'use' the system, [a defendant] must put the claimed invention into service, i.e., control the system and obtain benefit from it." *Id*. at 1286. Here, the documents Plaintiff cites to fatally contradict the plausibility of its own direct infringement allegations in at least two ways: (1) Cisco SAFE is not a definable "system" at all, but a reference framework uses to evaluate and guide network design (*See* Ex. 1. at 5-6), and (2) even if an infringing platform did exist, such a platform would be deployed and controlled by parties other than Cisco. *See De La Vega*, 2020 WL 3528411, at *6-7.

1. Plaintiff Does Not Allege Cisco "Makes," "Uses," or "Sells" Any Infringing Product or Thing

The Complaint fails as a matter of law because it fails to accuse any actual Cisco products, and further fails to allege that *any* infringing systems, from Cisco or otherwise, exists. Plaintiff relies heavily on excerpts and figures from a document entitled "SAFE Overview Guide: Threats, Capabilities, and the *Security Reference Architecture*" for the conclusory assertion that Cisco SAFE provides the "security subsystem," also described in the complaint as a "unified security management system," of the '799 Patent. *See* Ex. 1 (emphasis added); Complaint, ¶ 14. Despite Plaintiff's conclusory assertions parroting the claim language, the purported "accused instrumentality," Cisco SAFE is merely a conceptual reference model and not an actual "security subsystem." *See* Dkt. 1-2 at 4. This document, including the title and the excerpts Plaintiff specifically relies on, all make clear that Cisco SAFE is nothing but a *generic reference framework* representing broad design guidelines and industry best-practices. *See* Dkt. 1-2 at 1-2, 4; *see also* Ex. 1 at 6 ("SAFE is not a single answer. The model is a reference for common threats, risks, and policies across the business of a company."). The same is true for the only other document Plaintiff relies on in its claim chart. *See e.g.,* Dkt. 1-2 at 5-6 (claim chart relying only generic building blocks like "web security," "firewall," and "identity."); Ex. 2 at 11-1 ("Cisco SAFE advocates for

the continuous education of end-users on current threats and security measures."). Nothing in either document Plaintiff relies on plausibly indicates that Cisco SAFE is "made" or "used" by Cisco, or that Cisco "sells" the "security subsystem" of the patented claim— whether it is as an individual product or as a bundle of products. *See* 35 U.S.C. § 271(a); *see also Centillion Data Sys., LLC v. Qwest Communs. Int'l.*, 631 F.3d 1279, 1286-88 (holding as a matter of law that the accused infringer did not "make" or "use" the claimed system because it did not manufacture and combine all the components, or the put the system into service).

In fact, Plaintiff cannot point to even a single concrete system (from Cisco or from any other party) that infringes the '799 Patent, nor has it "presented anything other than speculation that such a network might actually exist." *Dynacore Holdings Corp. v. U.S. Philips Corp.*, 363 F.3d 1263, 1277 (Fed. Cir. 2004). Limitation (a) of the asserted claim requires "an open platform for receiving and executing security function software modules from multiple vendors for providing defense functions for protection of the host." The Complaint does not offer any explanation of what the accused "platform" is, what entity is using the system, what "vendors" are being integrated, what security software is being "receiv[ed] and execut[ed]" on the platform, *etc*. For example, the diagram included in Plaintiff's claim chart, implied to be depicting the infringing "platform," is just a stock diagram used to illustrate business flows and security capabilities of a generic fictional enterprise. *See* Dkt. 1-2 at 6. Instead, Plaintiff resorts to parroting claim language that Cisco SAFE provides a "platform," "software modules," and integration with "multiple vendors." *See generally* Dkt. 1-2. Without identifying any actual product or system, Plaintiff's attempts to rely on its identification of generic terms in Cisco SAFE documents do little more than raise "a theoretical possibility" of actual infringement. *Dynacore*, 363 F.3d at 1277. Ultimately, the Complaint's allegations "merely track the claim language" and are "insufficient to give rise to

a reasonable inference" that any infringing system exists. *Vervain, LLC v. Micron Tech., Inc.*, 2022 WL 23469, at *7 (W.D. Tex. Jan. 3, 2022) (citation omitted). Lastly, the Complaint alleges, without factual basis, that Cisco "has and continues to directly infringe … by having its employees internally test and use these exemplary Accused Instrumentalities." Complaint, ¶32. The Court should not blindly accept such "conclusory allegations or legal conclusions masquerading as factual conclusions." *Taylor v. Books A Million, Inc.*, 296 F.3d 376, 378 (5th Cir. 2002); *see also Chhim v. Univ. of Tex. At Austin*, 836 F.3d 467, 469 (5th Cir. 2016).

2. Direct Infringement of a System Claim Cannot Be Satisfied by Different Parties

Even if Plaintiff could plausibly allege the existence of any actual infringing systems, the Complaint nevertheless fails to advance any theory by which any direct infringement can be satisfied by Cisco. *See Ruby Sands LLC*, 2016 WL 3542430 at *4. The Cisco SAFE documents that Plaintiff relies on expressly indicate that Cisco SAFE is a reference tool for helping other companies design and evaluate their own networks. *See* Ex. 1 at 5 ("This Cisco security reference architecture features easy-to-use visual icons that help you design a secure infrastructure for the edge, branch, data center, campus, cloud, and WAN."). In other words, any hypothetical infringing network would be deployed and operated by third-parties, not Cisco. But various limitations of a system claim cannot be provided by different parties – each of the limitations must be satisfied by a single infringer. *See Centillion*, 631 F.3d at 1288. "Where, as here, the factual allegations are actually inconsistent with and contradict infringement, they are likewise insufficient to state a plausible claim." *Bot M8 LLC v. Sony Corp. of Am.*, 4 F.4th 1342, 1354 (Fed. Cir. 2021).

3. The Assortment of Other Cisco Products Cited in the Claim Chart Are Irrelevant

Because Cisco does not make, sell or use the "security subsystem" of the asserted patent, Plaintiff is forced to misrepresent other irrelevant Cisco products to satisfy the claim limitations,

such as CSA (Cisco Security Agent), CS-MARS, and Cisco IPS. Plaintiff's attempt to rely on these unrelated Cisco products is both factually implausible and legally insufficient.

First, CSA, and CS-MARS are all products that have not been sold or supported by Cisco for over 10 years.[1] Cisco retired CSA around 2010 and no longer sells or supports the product, meaning that the six-year statute of limitations would have already run even if those products did infringe (which Plaintiff does not plausibly allege). *See* 35 U.S. Code § 286. Plaintiff could easily have discovered this fact with a cursory investigation before relying on these long-discontinued products to cobble together its infringement allegations.

Second, Plaintiff has not plausibly alleged that these other Cisco products are relevant to the accused instrumentality or to the claimed system of the '799 patent. For example, Plaintiff's claim chart also cites to the SAFE Reference Guide stating that "Cisco SAFE…leverages the linkage between Cisco Security Manager and CS-MARS to simply management and to expedite troubleshooting and threat mitigation." Dkt. 1-2. at 3. But to the extent that Plaintiff is attempting to characterize these products as components of the accused instrumentality, the Complaint offers no explanation of how these unrelated products can be considered essential components of a Cisco SAFE "system" when Cisco SAFE is not a "system" at all—the documents specify that Cisco SAFE does not contain a specific design or set of instructions, and is not tied to any particular business or product. *See also* Ex. 1 at 6 ("SAFE is not a single answer…Obviously, the concerns of retailers are not the same as the needs of healthcare organizations.").

Third, Plaintiff fails to allege that these products can meet the claim limitations of the

[1] *See e.g.,* https://www.cisco.com/c/en/us/obsolete/security/cisco-security-monitoring-analysis-and-response-system.html (CS-MARS discontinued in 2011 and supported ended in 2016); https://www.cisco.com/c/en/us/obsolete/security/cisco-security-agent.html (CSA discontinued in 2010 and support ended in 2013).

asserted patent even assuming them to be components of a hypothetical Cisco SAFE "system." For example, Plaintiff alleges that CSA "checks the security policy for threats" and "combin[es] security policies." But simply combining security policies falls well short of a platform for "receiving and executing" security software that integrates products from "multiple vendors," as required by the claim. *See* '799 Patent at 19:50-52. Similarly, to the extent that Plaintiff relies on Cisco IPS products as providing "defense functions for protection of the host," that is also insufficient. *See* Dkt. 1-2 at 3, 5. Plaintiff fails to address substance of the claim, which is directed to an "open platform" capable of "receiving and executing" security software from "multiple vendors." '799 Patent at 19:50-52. Lastly, with respect to CSM or CS-MARS, the Complaint again entirely fails to allege provide users with the functionality for deploying a "unified security system" and "open platform" capable of integrating security software modules from multiple vendors, as required by the asserted claim. Therefore, to the extent that Plaintiff is accusing any of these other Cisco products, the Complaint simply fails to "articulate why it is plausible that the accused product infringes the patent claim." *Vervain*, 2022 WL 23469, at *7 (citing *Bot M8*, 4 F4th at 1354).

Finally, as discussed in the section above, direct infringement of a system claim requires that the accused infringer combines or puts into service the entire system, including all claim elements. *See Ruby Sands LLC*, 2016 WL 3542430 at *4. The various limitations of a system claim cannot be provided by different parties – each of the limitations must be satisfied by a single infringer. *See Centillion*, 631 F.3d at 1288. Cisco exercises no control over its customers' networks or security architecture. It cannot choose how its customers install, combine, or deploy its products. In other words, any hypothetical infringing network would be deployed and operated by third parties, not by Cisco.

In sum, Plaintiff "makes no factual allegations that even remotely suggest that" Cisco makes, uses, offers to sell, sells or otherwise provides a "security subsystem" as recited in Claim 14. *Ruby Sands LLC*, 2016 WL 3542430, at *4; *see also De La Vega*, 2020 WL 3528411, at *6-7; *Mosaic Brands v. Ridge Wallet LLC*, 2020 WL 5640233, at *4 (C.D. Cal. Sept. 3, 2020) (dismissing complaint for "failure to plausibly identify in the claim charts multiple limitations of Claim 1 of the [asserted patent.]"). Because the same documents Plaintiff relies on demonstrate that Plaintiff has no plausible direct infringement allegation, amendment would be futile and Plaintiff's Complaint should be dismissed with prejudice. *See De La Vega*, 2020 WL 3528411, at *6-7; *Ruby Sands LLC*, 2016 WL 3542430, at *4.

C. Plaintiff's Claims for Pre-Suit Indirect Infringement Should be Dismissed

Plaintiff also fails to plead any pre-suit knowledge of the '799 patent, as required to support a claim for indirect infringement (inducement or contributory infringement). *BillJCo, LLC v. Apple Inc.*, 583 F. Supp. 3d 769, 777-778 (W.D. Tex. 2022). Plaintiff similarly fails to plead that Cisco SAFE has no substantial non-infringing uses, as required to plausibly allege contributory infringement. *Id*. at 782 (dismissing contributory infringement claim because patentee "offer[ed] nothing to support [its] contention" that accused product had no substantial non-infringing uses).

V. CONCLUSION

For the foregoing reasons, Cisco respectfully requests that this Court dismiss Speech Transcription, LLC's Complaint with prejudice for failure to state a claim.

Dated: July 24, 2023

Respectfully submitted,

/s/ Krishnan Padmanabhan

WINSTON & STRAWN LLP
Krishnan Padmanabhan
California Bar No. 254220
200 Park Avenue
New York, NY 10166
Telephone: (212) 294-6700
kpadmanabhan@winston.com

ATTORNEYS FOR DEFENDANT CISCO SYSTEMS, INC.

CERTIFICATE OF SERVICE

I certify that the foregoing document was served upon all counsel of record via the Court's CM/ECF electronic filing system in accordance with the Federal Rules of Civil Procedure on July 24, 2023.

/s/ Krishnan Padmanabhan